UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/694,416	10/20/2000	Thomas Collins	20206-014(PT-TA-410)	1055

25696 7590 04/11/2003

OPPENHEIMER WOLFF & DONNELLY
P. O. BOX 10356
PALO ALTO, CA 94303

EXAMINER
SEAL, JAMES

ART UNIT	PAPER NUMBER
2131	23

DATE MAILED: 04/11/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/694,416	COLLINS ET AL.	
	Examiner	Art Unit	
	James Seal	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 September 2002* .

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-7 and 9-61* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-7 and 9-61* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

1. This action is in response to applicant's correspondence of 16 September 2002.

2. The IDS dated 16 September 2002 has been reviewed by the examiner and a signed copy is enclosed. IDS's received 8 December 1998, 11 April 2001, 26 June 2001 were signed and a copy returned to the applicant in the previous action.

3. The following amendments to the specification

- Col. 1, line 4
- Col. 2, line 64
- Col. 2, line 19
- Col. 3, line 23
- Col. 3, line 27
- Col. 3, line 56
- Col. 4, line 13
- Col. 4, line 32
- Col. 4, line 45
- Col. 4, line 41
- Col. 5, line 46
- Col. 5, line 52
- Col. 8, line 1
- Col. 8, line 62
- Col. 10, line 15
- Col. 10, line 25
- Col. 10, line 35

have been entered. The majority of the corrections included in this list, refer to obvious typos in the original patent. With regards to the replacement of "component" by "factor", although the applicants have shown no reason that these terms are used in the same sense, the examiner will allow the replacement as it does not seem to raise any other issues. Thus the examiner shall assume for the purpose of prior art that factor refers to prime factors of the composite number n that is p_1, p_2, p_3, ... p_k Although the original patent does not discloses "=" to means an "equivalence" relation (and thus may be replaced by "≡"), it is evident from the context in the original patent that this is what was meant.

4. Objection to application under 37 CFR 1.172 (a) as lacking the written consent of all assignees is withdrawn with the material provided Exhibit C of applicant's correspondence.

5. Receipt of formal drawings acknowledged.

6. Objection to the specification for new matter under 35 U.S.C. § 132 is maintained.

7. Objection to claim 3 is withdrawn with amended version.

8. Rejection of claims 7, 8, and 13 under 35 U.S.C. § 101 for lack of utility is withdrawn. With the cancellation of claim 8 and the amendment to claims 7 and 13 the issue is now moot.

9. Rejection of claim 8 and 13 under U.S.C. § 112 first paragraph for lack of enablement, is withdrawn, due to cancellation of claim 8, and amended claim 13.

10. Rejection of claims 26-30 under 35 U.S.C. §112 second paragraph is withdrawn with the amendments to these claims.

New Matter Objection

11. The amendment filed 16 September 2002 is objected to under 35 U.S.C. 132 because it introduces new matter into the disclosure. 35 U.S.C. 132 states that no amendment shall introduce new matter into the disclosure of the invention. The added material which is not supported by the original disclosure is as follows:

12. As per the amendment Col. 4, line 6 the replacement of the phrase "*using* the RSA scheme" "... using a large (many digit) n much faster than heretofore possible", "*extending* the RSA scheme" "... using a large (many digit) n much faster than heretofore possible" . The support relied upon by the applicant is Col. 3, lines 20-26, Col. 4, line 6-12, 32-34 and 52-56. The examiner interprets the first to mean that the present invention is capable of using the RSA scheme to perform encryption and decryption operation using a large (many digit) n much fast than hereforth possible, that is, using an existing system. The replacement discloses using a new system (an extended RSA) for accomplishing this task. The applicant offers support from Col. 3, lines 20-26 deal with extending the computational speed without any mention of "using a large (many digit) n or an existing RSA system", Col. 4, line 6-12 is the same paragraph that is being amended. Column 4, lines 32-34 discloses a system that employs parallel processing which does not support the change and Column 4, line 52-56 refers to the CPU breaking the encryption/decryption into sub-tasks. None of Attention:Attention:these references are directed atFinal Rejection going from an existing RSA system to an extended system and using the extended system "... using a large (many digit) n much faster than heretofore possible" with "extending the RSA scheme". For that

reason the examiner does not believe the change is supported and would constitute new material.

13. With regards to the amendment Column 5 line 30, "developed and checked to ensure that each $(p_i - 1)$ is relatively prime to e" the applicant provides support from Column 2, lines 5-10, Col. 3 line 42, col. 4, line 41, Col. 5, line 39, Col. 10, line 65 and col. 11, lines 8-9. Col. 2, lines 5-10 refers to only the standard two prime RSA case. Col. 3, line 42 discloses only $n = p_1 p_2 \ldots p_k$ but no mention of $(p_i - 1)$ relatively prime to e. Col. 4, line 41 discloses $n = p_1 p_2 \ldots p_k$ but no mention of $(p_i - 1)$ relatively prime to e. Col. 5, line 39 $d = e^{-1} \bmod [(p_1 - 1)(p_2 - 1) \ldots (p_k - 1)]$ but no mention of $(p_i - 1)$ relatively prime to e. Col. 10, line 65 discloses where is is relatively prime to $(p_1 - 1)(p_2 - 1)$. The amended claim 1, discloses support of changes of $(p_1 - 1)(p_2 - 1)$ to $[(p_1 - 1)(p_2 - 1) \ldots (p_k - 1)$ using Col. 5, line 30. Col. 11, lines 8-9, discloses that d is the multiplicative inverse to e, and does not address $(p_i - 1)$ relatively prime to e. Further none of the sections recited for support disclose the step of "checking" that each $(p_i - 1)$ is relatively prime to e.

14. With rgards to amendment to Col. 5, line 52, no support can be found for digital signature in the original. Claim 9 was quoted as support. Claim 9 does mension a signed message M_{As} however claim 10 refers to M_{As} as "said *signal message* word signal" which makes it unclear if this is support for a digital signature. See means plus function rejection of claim 9. Amendment contains matter no clearly supported by original patent and therefore constitutes new matter and should be taken out.

15. With regards to the amendment to the specification at Column 6, line 24. This amendment to the specification, request that $i \geq 2$ in the original patent with

$2 \leq i \leq k$ where k is the number of primes in n. The latter is certainly satisfied by i = k = 2, but k must always be equal to or greater than *three* as specified in the original patent (cf. Col. 5, line 31-32), thus the two statements contradict one another. If the former is what applicant wants, then applicant should supply support for this in the specification or it would constitute new matter.

16. With regards to Col. 6, line 65, in the original patent the sentence reads:

> "In generalized form, the decrypted message M can be obtained by the same summation identified above to obtain the ciphertext from its contiguous constituent sub-tasks C_i."

In the amended version the sentence reads

> "in generalized form, the ciphertext C (i.e., encrypted message M) can be obtained by a recursive scheme as identified above to obtain the ciphertext C form its contiguous constituent sub-tasks C_i."

The examiner notes that the first version reads "the decrypted message M can be obtained" while the second version reads "the ciphertext C can be obtained" which are two distinctly opposite functions. The first version *summation* is required wherein the second version *iteration* is required. Support for the second version is cited Column 6, lines 1-4; line 26-35; 40-53, and 67 and in particular it would appear that the applicant is making use of "however, it is found that they can most expeditiously be combined by a form of the Chinese Remainder Theorem (CRT) using, preferably, a recursive scheme." The examiner observes that the use Chinese Remainder Theorem (a summation process) is the focus of the discussion with iteration is given as *the preferred* method for carry out this function, the proposed iteration scheme being given lines 31-39. What follows next lines 40-64 is the standard decomposition for using the CRT for recovering

M, then version 1 is given which would be mathematically logical followed by the CRT first equation Column 7 providing the summation process to obtain M. The first sentence at the top of Column 7 again states that the recursive form of the CRT referring to Column 6, lines 31-39 is preferable for greater speed but then returns to finish with the summable CRT. The examine fails to see where any support has been provided for the second version.

The examiner notes from page 39 second paragraph, of applicant's correspondence, support for amendment at Col. 7, line 1 is given as Col. 2, lines 32-34 and 40, Col. 3, lines 22-26, Col. 4, lines 32-34, Col. 6 line 38 and Col. 7, lines 56-58, whereas no support is provided for the amendments regarding Col. 7, line 17 and Col. 7, line 52. As far as the examiner can see, the quoted references do not provide support for Col. 7 line 1 which is a statement of the standard CRT; however, they do not appear to support amendments Col. 7, line 17 (a special case of the CRT) or Col. 7, line 52 (which involves the labels in Figure 1) either. The examiner also notes no support for the amendment to the specification at Col. 9, line 24. The examiner asked that proper support be supplied for these amendments.

Applicant is required to cancel the new matter in the reply to this Office Action.

17. Claim 8 is cancelled without prejudices.

18. Amended claims 1-7, and 9-13 have been entered.

19. Amended new claims 14-61 have been entered

20. Claims 1-7 and 9-61 are pending.

Claim Objections

21. Claim 4 objected to because of the following informalities:

In line 18 of claim 4, lcm (p1-1, p2-1, ... pk – 1) should read lcm (p_1-1, p_2-1, ... p_k – 1) that is, 1, 2, 3, ..., k should appear as subscripts.

22. Claim 35 is objected to because of the following informalities. In line 5, *p*k should be p_k

Appropriate correction is required.

Claim Rejections - 35 USC § 112

23. Rejection of claims 26-30 under 112 second paragraph is withdrawn with amendments to claims

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

24. Claim 1 rejected under 35 U.S.C. 112, first paragraph, as containing subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

25. Claims 1-2, 18-19, 32-33, 37, 42-49, 56--61 recites "developing k distinct random prime numbers p_1, p_2, ... p_k where k is an integer greater than 2; providing a number e relatively prime to (p_1 – 1) (p_2 –1) ... (p_k-1)". The patent as originally filed does not disclose such a condition for k ≥ 3. The only reference found in the original reference is given on column 5, line 33, which recites "Then, three or more random large, distinct primes numbers, p_1, p_2, ... p_k are developed and checked to ensure that *each is relatively prime* to e", which alleges the primes such be relatively primed to e, and thus does not supported by

the original patent. Claims 1-2, 18-19, 32-33, 37, 42-49, and 56—61 are rejected under new matter.

26. Claims 3, 4-6, 9-12, 14-19, 28-37, 40-41 recites "developing k distinct *random* prime numbers p_1, p_2, ... p_k where k is an integer greater than 2; providing a number e relatively prime to lcm ($p_1 - 1$, $p_2 - 1$, ..., p_k-1)" or the lowest common multiplier. The patent as originally filed does not disclose such a condition for $k \geq 3$ as disclosed above. The only reference found in the original reference is given on Column 5, which recites "Then, three or more random large, distinct primes numbers, p_1, p_2, ... p_k are developed and checked to ensure that each is relatively prime to e". The applicant has not provided support for this new limitation either from the original patent are from the RSA patent. Claims 3, 4-6, 9-12, 14-19, 28-37, 40-41 are rejected under new matter.

27. Claims 1-61 rejected under 35 U.S.C. 112, first paragraph, as containing subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

28. Claims 1-61 now recite "developing k distinct *random* prime numbers p_1, p_2, ... p_k where k is greater than 2... ". The term *random* with regards to the primes p_1, p_2, ... p_k is cited once in the original patent Column 5, line 31 and does not appear in the RSA patent with regards to the primes. Claims 1-61 are rejected under new mater.

29. As the applicant points out in the last paragraph of page 46 and the top of page 47 of his correspondence, it is clear that the applicant now believes that "The *randomness* and distinctness attributes of the k prime numbers will materially improve the security in any

cryptographic system with RSA public key encryption." If this were the intent of the original patent, the original patent does not support this view.

30. Claim 7 and 13 rejected under 35 U.S.C. 112, first paragraph, for lack of written decryption.

31. In claims 7 and 13, applicant claims a method "cryptographically processed with an RSA public key encryption ... developing k factors of a composite number n, the k factors being distinct random prime numbers and k an integer larger than two ... through a relationship of the form

$$C \equiv a_e M^e + a_{e-1} M^{e-1} + \ldots + a_0 \pmod{n}$$

where e and a_e , a_{e-1}, ... , a_0 are numbers; and deciphering the received ciphertext word signal C at an intended recipient with knowledge of the k factors. The applicant provides no support for how this is to be done in the specification or drawings. Claims 7 and 13 are rejected.

32. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

33. While applicant may be his or her own lexicographer, a term in a claim may not be given a meaning repugnant to the usual meaning of that term. See *In re Hill*, 161 F.2d 367, 73 USPQ 482 (CCPA 1947). The "relationship" in claims 7 and 13 is used by the claim to mean "an RSA public key encryption." When a message is said to be cryptographically processed with an RSA public key encryption, the standard interpretation of this phrase would be

$$C \equiv M^e \pmod{n}$$

with decryption carried out as follows

$$M \equiv C^d \pmod{n}$$

Such that e and d are related as follows

$$ed \equiv 1 \bmod \phi(n)$$

This is not the "relationship" being claimed as an RSA public key encryption.

34. Regarding amended claim 9, the word "means" is preceded by the word(s) " $M_{1s} \equiv M_1{}^{d_1} \bmod n_1$ " in an attempt to use a "means" clause to recite a claim element as a means for performing a specified function. However, since no function is specified by the word(s) preceding "means," it is impossible to determine the equivalents of the element, as required by 35 U.S.C. 112, sixth paragraph. See *Ex parte Klumb*, 159 USPQ 694 (Bd. App. 1967).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

35. Claims 1-7, 9-61 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rivest et. al. (US 4,405,829 A) henceforth RSA, and further in view of Rivest et. al. A Method for Obtaining Digital Signatures and Public-key Cryptosystem, Communications of the ACM, 21(2) February 1978, henceforth Rivest and further in view of Knuth, The Art of Computer Programming vol 2 page 179.

36. As per amended claim 1, the limitation of a method for processing messages in a communication system with RSA public key encryption an alternative embodiment of the present invention (see Figure 6, Abstract line 1 of Column 4, lines 15 through Column 5, lines 11, RSA), such that three or more primes $p_1, p_2, p_3, \ldots, p_k$ are generated, such that $k > 2$ (Column 13, lines 30-31) then using the present invention (Column 13, line 29) provided and e relatively prime to $\phi(n)$ (Column 13, lines 42-44), $\phi(n) = (p_1 - 1)(p_2 - 1)(p_3 - 1)\ldots(p_k - 1)$, that is, relatively prime to $(p_1 - 1)(p_2 - 1)(p_3 - 1)\ldots(p_k - 1)$ and generating from the product of these primes and integer n which will be the resulting modulus n (Column 13, line 30-31, line 34) using the provided e and n together with a message M where $0 \leq M \leq n-1$ (Column 4, line 26), and the RSA encryption algorithm $C \equiv M^e \bmod n$ (Column 4, line 59, RSA) to generate a cipher text C, decrypting C at the intended recipient (Column 6, 29-31) having available to it

37. With regards to what the applicant regards as his invention and how it differs from the RSA patent, we consider first applicant's comments page 46 of amendment. The recitation in claim 1 includes developing k distinct random prime numbers $p_1, p_2, p_3, \ldots, p_k$, where k is an integer greater than 2, and further includes the fact that the modulus n is a composite number equaling the product $p_1p_2p_3 \ldots p_k$. Namely, claim 1 recites that k . 2 and the k primes numbers are random and distinct. Moreover, claim 1 receites that the modulus n is provided from a product of the k prime numbers. Contrast this (claim 1) recitation with selecting a modulus n and then factoring n to the k prime numbers. It is clear from this that the applicant believes that RSA teach selecting a modulus n and then factoring n as oppose to selecting k distinct random primes.

38. RSA patent does not disclose the method by which they choose primes; however, on page 123, column 2 at the beginning of section B, Rivest states "each user must (privately) choose two large random prime number p and q to create his own encryption and decryption keys" Thus it is clear that Rivest does intent to use large random primes for RSA cryptosystem in general. Rivest states to protect against sophisticated factoring algorithms, each prime should *differ in length by a few digits* (Rivest, page 124 third paragraph). Thus Rivest teaches randomness and distinctness for security of the primes for RSA cryptosystems.

39. RSA patent recites a different embodiment (Column 13, lines 30-31) in which the modulus n is a product of three or more primes (not necessarily distinct primes). RSA further goes on to state that decoding may be performed modulo each of the prime factors of n (thus breaking the calculations into a series of subtacks involving the factors of n and not n) and then combining the results using "Chinese remaindering" (that is the Chinese remainder theorem henceforth CRT). However, only in the case of distinct primes can the decoding problem be performed using the CRT. In the case of non-distinct primes one would need in addition Hensel's Lemma (or a generalization by Hensel of p-adics, see Knuth vol 2, page 179). Thus it is clear that the RSA patent is referring to the case of distinct primes. Claim 1 is rejected.

40. As per claim 2, the RSA patent teaches that in any RSA public key cryptosystem, may be implemented in an alternative embodiment of the present invention by making n the product of k random and distinct primes, such that, the decryption of ciphertext C should be accomplished by $M \equiv C^d \bmod n$ is disclosed Column 13, lines 44-46 and d is chosen as the

multiplicative inverse of e such that ed ≡ 1 mod L, L = least common multiple, which in the case of k primes is L = lcm { $p_1 - 1$, $p_2 - 1$, ...$p_k - 1$ }) (Column 5, lines 1-15, Column 13, line 30-31). Claim 2 is rejected.

41. As per claim 3, RSA patent teaches that in any RSA public key cryptosystem may be implemented in an alternative embodiment of the present invention with the limitation of j communicating terminals on a communication system, with encrypting key $E_i = (e_i, n_i)$ and decryption keys $D_i = (d_i, n_i)$ i = 1, 2, ... j, (Column 8, lines 22-27) wherein for each terminal i, e_i, d_i, and n_i are defined as in claims 1 and 2 (see above) wherein the message M_i corresponding to a number representative of a message-to-be-transmitted from the ith terminal and in particular terminal 1 transmits a message M_1 to terminal 2 by breaking the message M into blocks M" where $0 \leq M_1" \leq n_2 - 1$ (Column 4, lines 31-35; Column 8, line 39) message to ciphertext using $C \equiv M_1"^{e2} \bmod n_2$ (Column 8, line 56). Claim 3 is rejected.

42. As per claim 4, the RSA patent teaches that in any RSA public key cryptosystem, may be implemented in an alternative embodiment of the present invention by making n the product of k random and distinct primes, such that, the limitation that the decryption of the ciphertext C between two terminals (as defined in claim 3) is decrypted according to $M' \equiv C^d \bmod n$ (where d and n are defined as above) and where M' corresponds to the decoded ciphertext block is disclosed (Column 8, line 43). Claim 4 is rejected.

43. As per claim 5, the limitation of a communication system incorporating the encryption of messages as claim 3 and the receipt and decryption of messages as claim 4 form a *first* (or transmitting) terminal to a second terminal and are therefore rejected on grounds analogous to those used to reject claims 3 and 4.

44. As per claim 6, the limitation of a communication system incorporating the encryption of messages and the decryption of messages from a second (transmitter) terminal to a first terminal (receiver) and a blocking means (Column 4, line 33) and are therefore rejected on grounds that the limitations of claim 6 combine the limitations of claims 3 (an encoder for encrypting messages to be transmitted) and 4 form (decoding messages encrypted in the manner of three) and are rejected in view of the same art of record.

45. Claim 8 is cancelled.

46. As per claims 9 and 10, the limitation of sending signed messages between terminals is disclosed by Rivest Column 5, lines 18-50 and Column 8 lines 56-67. Claims 9 and 10 are rejected.

47. As per claim 11, the limitation that the communication system is comprised of stations capable of generating ciphertext is disclosed by Rivest Column 8, lines 33-39 and Column 10, line 28-34. Claim 11 is rejected.

48. As per claim 12, the limitation that such stations transmit ciphertext is disclosed by Rivest Column 8, lines 33-39, Column 10, lines 11-24, lines 28-34, and Figure 4. Claim 11 is rejected.

49. As per claim 13, the limitations that a communication system has stations in the manner of claim 11 for encryption/decryption messages which is carried out according to claims 7 and 8 is therefore rejected on the grounds analogous to those used to reject claims 7, 8 and 11.

50. As per claims 14 and 15, a method of processing messages by *selecting* a public e which is used with the relationship $C \equiv M^e \bmod n$ (claim 14) and (claim 15) *establishing* a

private key portion $d \equiv e^{-1} \bmod L$ respectively is disclosed by Rivest Column 6, lines 21-37. Claims 14 and 15 are rejected.

51. As per claim 16, a method of processing messages selecting a public key e and establishing a private key $de \equiv 1 \bmod L$ where n is a product of 3 or more *distinct* primes and decoding ciphertext using the relationship $M \equiv C^d \bmod n$ is disclosed by Rivest Column 6, lines 21-37 and Column 13 lines 29-31, lines 41-43. Claim 16 is rejected.

52. As per claim 17, the limitation $M \equiv C^d \bmod n$ is disclosed by Rivest Column 13 line 46. Claim 17 is rejected.

53. As per claim 18, selecting a public key e and corresponding private key $d \equiv e^{-1} \bmod \phi(n)$ and encrypting M with the private key produces a signed message M_s is disclosed by Rivest Column 8 lines 56-67. claim 18 rejected.

54. As per claim 19, the limitation that the signed message can be verified by the public key is disclosed by Rivest Column 9, line 3. Claim 19 rejected.

55. As per claims 20-23, the limitations of a multiprime RSA cryptosystem n = pqrs... whereby the speed of the cryptographic process is increased is disclosed by Rivest Column 13, line 33. Rivest discloses the use of the CRT, which because of its mathematical form allows the breaking up of the decryption process into a series of subtasks ($M_p \equiv C^d \bmod p$; $M_q \equiv C^d \bmod q$; $M_r \equiv C^d \bmod r$; and $M_s \equiv C^d \bmod s$ ...). This puts the calculation in terms of subtask which are then automatically in a form to utilize parallel processing in the calculation and because the primes used in each subtask are small, increased speed is a consequence. Claims 20-23 are rejected.

56. As per claims 24, 25, 28, 30, and 32, in as far as the examiner understands the limitation, "fewer computational cycles" for a multiprime RSA cryptosystem, is disclosed by Rivest as a results of the CRT as discussed above. With smaller primes, the necessary computational cycles would also be less, for example using the Euclidean algorithm or the CRT. Claims 24, 25, 28, 30, and 32 are rejected.

57. As per claims 26, 27, 29, 31, and 33, in as far as the examiner understands the limitation, "faster than heretofore possible" for a multiprime RSA Cryptosystem is disclosed by Rivest as a results of the CRT as discussed above. If the number of computational cycles is fewer that would imply that the calculation are completely faster. Claims 26, 27, 29, 31, and 33 are rejected.

58. As per claims 34-39, in as far as the examiner understands the limitation, a "method compatible with RSA" with the multiprime RSA is disclosed by Rivest. Rivest would allow a standard two prime RSA cryptosystem to communicate with a multiprime RSA cryptosystem as only the public keys (e, n) are used for encryption by the other party machine and no use of the factorization is used in the process. Claims 34-39 rejected.

59. As per claims 40-41, the limitation of a cryptographic method for local storage of data by a private key is disclosed by Rivest Column 6 lines 50-57 and grounds in claims 14 and 15. Claims 40-41 rejected.

60. As per claim 42, the limitation of a communication system with a plurality of stations over a communication link (channel) is disclosed by Rivest Abstract.

61. As per claim 43, the limitation of a system for processing message by encrypting a first message $C \equiv M^e \bmod n$ and also being able to decrypt a second encrypted message C' into M' is disclosed by Rivest (see Figure 4). Claim 43 is rejected.

62. As per claims 44 and 45, the limitation of breaking the encryption/decryption into subtasks is a consequence of the application of the CRT which Rivest discloses in Column 13 line 33. Claims 44 and 45 rejected.

63. As per claim 46-49, the limitations of data bus (Figure 3), processor(Figure 3), memory (Figure 1&3), exponentiator (Figure 3, element 22) parallel processing (Column 13, line 33) is disclosed by Rivest Column 9, lines 6-58; Figure 3. DES implementation for session keys is disclosed by Rivest (Column 3, lines 23-30 and Column 1, lines 42-45, Column 14, lines 26-28). Claims 46-49 rejected.

64. As per claims 50-55, limitations involving subtasks is a consequence of the CRT which breaks up the decryption process ($M_p \equiv C^d \bmod p$; $M_q \equiv C^d \bmod q$; $M_r \equiv C^d \bmod r$; and $M_s \equiv C^d \bmod s$ ...) into subtask (Column 13, lines 31-34) disclosed by Rivest. Claims 50-55 are rejected.

65. As per claims 56-61, it would be inherent that Rivest would provide a means of key development or key generation in order to prevent degrading of security of the encryption system from overuse of keys. Claims 56-61 are rejected.

66. Claims 7 and 13 are rejected in view of RSA patent US 4405829 A) and Rivest et. al. A Method for Obtaining Digital Signatures and Public-key Cryptosystem ACM) and further in view of Schwenk US 5835598 A.

67. As per claims 7 and 13, the limitation of processing encrypting messages M where $0 \leq M \leq n-1$ into ciphertext C, and such that the ciphertext is generated from the plaintext as follows:

$$C \equiv a_e M^e + a_{e-1} M^{e-1} + \ldots + a_0 \bmod n$$

where e, a_e, a_{e-1}, ... a_0 are numbers is disclosed by Rivest Column 13, lines 36-39. Claim 7 is rejected.

68. Schwenk discloses encryption and decryption using a form above using the factors and coefficients and the CRT to assemble the results (Column 2, lines 25-67and Column 3, lines 1-35.

69. Claims 1-6, 11-12, 14-17, 20-31, 34-36, 38-44, 50-57, 60-61 rejected under 35 U.S.C. 102(b) as being anticipated by Vanstone and Zuccherato (*Using four-prime RSA in which some bits are Specified*, Electronic Letters, 30(25), 16 August 1994).

70. Vanstone et. al. discloses an device for reducing key size for transmission to a group of users in a communication system using 4 primes RSA for increased speed and security (Vanstone et. al., column 1, page 2118,). Vanstone system is in response to the recently advances in factoring which make integers n, in the range 2^9 = 512 bits insecure and suggests going to 2^{10} = 1024 bits with 4 randomly selected primes, each prime contains about 250 bits in both cases (Column 1, first four sentences). There is nothing in the Vanstone method which precludes extending to more bits or more primes in order to address future security needs. Vanstone selects random primes even though he makes bit assignments in an expanded product. Vanstone further discloses use of the CRT for decryption ($M = C^d \bmod n$, $0 \leq M \leq n - 1$), which because of its mathematical form of breaking the decryption process into a series of subtasks ($M_p \equiv C^d \bmod p$; $M_q \equiv C^d \bmod q$; $M_r \equiv C^d \bmod r$; and $M_s \equiv C^d \bmod s$) allows implementation of parallel processing in the calculation. Furthermore the form of the CRT indicates that the primes are distinct. Claims 1-6, 11-12, 14-17, 20-31, 34-36, 38-44, 50-57, 60-61 rejected.

71. The examiner wishes to thank the applicant for pointing out the typo, that the rejections under Nemo and Slavin should have been under 102 (a) not 102(e). The rejection stands now as a 103(a) with the amendments to the claims. If the applicant wishes to swear behind these references, he should do so.

72. Claims 1-6, 9-12, 14-31, 34-36, 38-44, and 50-61 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nemo (RSA Moduli Should Have 3 Prime Factors), and further in view of Rivest et. al. (A Method for Obtaining Digital Signatures and Public-Key Cryptosystem). The Nemo article was submitted in the original Collin's application, and although no publication date mentioned in the parent case, the footnote at the bottom of the first page of the article, list a date of August 1996.

73. Nemo discloses an apparatus/method for use in networks and smartcard of using 3 primes (three primes) RSA for increased speed (section 4.1) and security (section 5) applicable to networks (section 4.2) using digital signature for validation (section 4.2, last paragraph and section 6) in a standard digital architecture (section 4.1). The speed increase due to the CRT and smaller moduli see Section 3.1 and 4, in particular parallel processing using subtasks (see especially 3.1).

74. Nemo does not discuss how to choose the primes in his article; however, Rivest article teaches that RSA public key cryptosystem should use distinct and random primes. Modivation for distinct random primes is to be found in the speed and security of such a method. Claims 1-6, 9-12, 14-31, 34-36, 38-44, 50-61 are rejected.

75. Claims 1-6, 11-12, 14-17, 20-31, 34-36, 38-44, and 50-61 are ejected under 35 U.S.C. 103(a) as being unpatentable over Itakura and Nakamura, A Public-Key Cryptosystem Suitable for Digital Multisignatures, NEC Res. & Develop. No 71, October,

and further in view of Rivest, A Method for Obtaining Digital Signatures and Public-key Cryptosystem.

76. Itakura et. al. discloses an apparatus/method for cryptographic communications extending the two prime public key encryption to using three primes (page 4, Column 1)using 3 randomly selected distinct primes RSA for which the encryption is carried out $C \equiv M^e \bmod n$ and $n = pqr$ and $ed \equiv 1 \bmod (p-1)(q-1)(r-1)$ where e is relatively prime to and smaller than (p-1)(q-1)(r-1) (page 4 and where decryption is carried out by $M \equiv C^d \bmod n$ where $0 \leq M \leq n-1$ and capable of performing one or more digital signatures per document $S \equiv M^d \bmod n$ (See page 4 section 3) for increased speed and security of digital multisignature applicable to public-key cryptosystem in conjunction with a communication system for a plurality of users (network, see Figure 1, see Abstract Electronic mail). Itakura et. al. use a random number key generator to develop keys (Figure 1, section 3.1) Claims 1-6, 11-12, 14-17, 20-31, 34-36, 38-44, 50-61 rejected

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Claim Rejections - 35 USC § 102

77. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

Claims 1-6, 9-12, 14-31, 34-36, 38-44, and 50-61 are rejected under 35 U.S.C. 102(a) as being anticipated by Salvin.

78. Salvin discloses a method of encrypted communication (Abstract) using four prime RSA $n = p_1xq_2,xp_1xq_2$, in which the four primes are selected at *random* and all of which *all are different values* (Column 7, lines 35-67in particular lines 37-38)and corresponding public and private keys e and d (see figure 3, Column 4, lines 31-38 applied to a network with a plurality of users (Figure 1). Salvin further discloses the use of the CRT to speed up the 4 prime decryption (Column 9, lines 44-47) whose speed is inherent from the breaking up the modular exponentiation into smaller primes and parallel subtask.

Response to Arguments

Applicant's arguments filed 16 September 2002 have been fully considered but they are not persuasive.

79. Applicant Comments directed at the random distinct choice of primes and whether n is factored into its factors or if the factors have been selected ahead of time

have been addressed above with regards to RSA patent have been addressed above. With regards to parallel subtasks, Knuth the Art of computer programming should apply.

80. With regards to Vanstone article on 4 primes, the applicant is reminded that the primes are selected at random but the bits are optimized thus meeting the applicant's criterion of randomness.

81. Nemo is still applied as art.

82. Applicant argues that comments sweept at once over the entire group of claims 1-7 and 9-61 however it should be noted that only certain claims are addressed by each reference and each of these references are applied to different arts. Applicant argues that prior art such as Slavin and Itakura do not meet his random criternion, however discussion particular in Slavin do point out randomness as a teaching. Even in the case that they did not Rivest addresses these issues directly. Applicant's arguments about subtasks and parallel computation for speed have been address above in the discussion of the CRT and Column 13 RSA patent. However, Knuth's Art of computer Science discusses the concept of speed, parallelism and the Chinese Remainder Theorem. The statement that Slavin teaches away from multiprime as that what the teaching of his patent concern. However, looking at Column 7, as directed by applicant, the second on the limitation of RSA seems to teach against the traditional two prime RSA for speed and security. In the preferred embodiment he state (lines 60) "Instead of two primes as used in the RSA technique, we use four randomly selected primes p_1, q_1, p_2, q_2, all of different values and We calculate

$N = p_1 q_1 p_2 q_2$

The same teachings of the applicant.

Double Patenting

83. Double patenting withdrawn with adminments.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to James Seal whose telephone number is 703 308 4562. The examiner can normally be reached on M-F, 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gail Hayes can be reached on 703 305 9711. The fax phone numbers for the organization where this application or proceeding is assigned are 703 746 7239 for regular communications and 703 746 7240 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703 308 3900.

jws
February 11, 2003

GAIL HAYES
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100